Windows Server 2016 Debug -Ympäristö

HAMK
HÄMEEN AMMATTIKORKEAKOULU
HÄME UNIVERSITY OF APPLIED SCIENCES

Ammattikorkeakoulututkinnon opinnäytetyö

Hämeen ammattikorkeakoulu Riihimäki, Tieto- ja viestintätekniikan insinööri

Kevät, 2018

Tuomas Jaakkola

HÄMEEN AMMATTIKORKEAKOULU
HÄME UNIVERSITY OF APPLIED SCIENCES

Tieto- ja viestintätekniikka
Riihimäki

Tekijä Tuomas Jaakkola **Vuosi** 2018

Työn nimi Windows Server 2016 Debug -ympäristö

Työn ohjaaja Teemu Järvenpää

TIIVISTELMÄ

Tein opinnäytetyöni Windows Server 2016 Debug -ympäristöstä, jonne asensin palvelimen yleisimmät roolit ja testasin, kuinka Windowsilla toimii containerit. Palvelimen rooleja olisivat muun muassa Active Directory, DHCP, DNS ja WSUS. Verkkoympäristössä käytin arkikäyttöistä 4G-reititintä, joka toimi yhdyskäytävänä ISP-päähän. Hyödynsin Active Directory -osiossa arkikäyttöistä pöytäkonetta, joka toimi Client-laitteena.

Valitsin aiheekseni Windows-palvelimen debug-ympäristön siksi, että olen kiinnostunut verkko- ja palvelintekniikasta, mutta myös siksi, että koululla emme käyneet läpi niin kattavasti Windows-palvelinympäristöä ja -rooleja. Myös kesän 2017 harjoittelupaikalla Windows-palvelinten osuus jäi vähälle. Tällä tavoin täydennän omaa osaamistani alueella, joka sekä kiinnostaa minua että hyödyttää minua työelämässä.

Sain hyvän yleiskuvan Windows Serverin hallinnoimisesta ja Containereiden luomisesta ja ajamisesta opinnäytetyön myötä. Palvelimen käyttöönotto ei itsessään ole hankalaa, jos tarvitsee hallinnoida vain käyttäjiä ja resursseja Active Directoryssa. Tällä hetkellä Windows Server Containerit ovat kuitenkin melko alkuvaiheessa, mutta kokeneempi ohjelmisto- tai WEB-kehittäjä saisi varmasti enemmän niillä aikaan. Linux Containereiden ajaminen oli huomattavasti helpompaa minulle.

Avainsanat Container, Palvelimet, Windows Server 2016.

Sivut 28 sivua

HÄMEEN AMMATTIKORKEAKOULU
HÄME UNIVERSITY OF APPLIED SCIENCES

Communication and Information Technology
Riihimäki

Author Tuomas Jaakkola **Year** 2018

Subject Debug environment of Windows Server 2016

Supervisor Teemu Järvenpää

ABSTRACT

For my project, I decided to work in a Windows Server 2016 debug environment, where I installed typical roles and programs, and tested how containers worked. The server's roles would for example include: Active Directory, DHCP, DNS and WSUS. I also created a network environment with my 4G-router to provide a connection between the Active Directory Server and the clients. The hardware of the server was a potential limiting factor since they do not consist of server hardware. For the Active Directory part, I used my PC as a client device.

I chose the Windows Server 2016 debug environment as the subject for my thesis, because I am interested in networking and servers in general, but also because we did not have that extensive training on Windows Servers at the university and during my internship in the summer of 2017, I did not get to work a lot with Windows Servers. By writing my thesis on this subject, I expanded my knowledge on the subject that both interests me, but also will help me in my future career.

I got a good overview on Windows Server Administration and on creating and running Containers along the thesis. Deployment of the server itself is not that difficult if the requirement is to administer users and resources using Active Directory. Windows Server Containers are still quite tricky, and it would require more knowledge on WEB-development to create something useful with them. Running Linux containers were considerably easier for me.

Keywords Container, Servers, Windows Server 2016.

Pages 28 pages

SISÄLLYS

SANASTO

Active Directory on käyttäjätietokanta ja hakemistopalvelu, jonne tallentuu tietoa verkon käyttäjistä, tietokoneista ja resursseista (Wikipedia 2017a).

Container Host, joka on fyysinen tai virtuaalinen laite, jolla ajetaan yhtä tai useampaa containeria (Microsoft Corporation 2016a).

Container Image, esimerkiksi ohjelma, joka on pakattu ajettavaksi Containerissa (Microsoft Corporation 2016a).

Container OS Image on ensimmäinen mahdollisesti monista Image layereista, josta container koostuu. Tämä kuva antaa käyttöjärjestelmä ympäristön, jossa Container Image toimii. Container OS Image on muuttumaton, täten siihen ei pysty tekemään muutoksia. (Microsoft Corporation 2016a.)

Container Repository. Joka kerta, kun Container Image luodaan, tämä ja siitä riippuvaiset osat säilötään local repositoryyn (paikalliseen säiliöön). Täten näitä Container Imageita voidaan käyttää monta kertaa Container Host -laitteella. (Microsoft Corporation 2016a.)

DHCP on automaattinen tapa jakaa ja päivittää IP-osoitteita ja muita konfiguraatioita verkossa (Microsoft Corporation 2003).

DNS eli Domain Name System. DNS:n avulla voidaan muuntaa IP-osoite merkkijonoksi. (Microsoft Corporation 2017a.)

Docker on container-alusta, jolla voidaan nopeasti luoda testiympäristö tietylle prosessille tai ohjelmalle (Vaughn-Nichols 2018).

Docker File on Dockerin käyttämä tiedosto, joka sisältää ohjeet, miten koota Docker Image (Docker Inc. 2017).

Docker Image on tiedosto, jota Docker käyttää luodakseen testiympäristönsä. Näitä voidaan joko luoda itse tai hyödyntää valmiita imageja. (Docker 2018.)

Domain eli toimialue. Toimialueella tarkoitetaan joukkoa tietokoneita ja laitteita, jotka ovat kytketty samaan verkkoon, joille on määritetty erinäisiä oikeuksia (Beal 2017).

Domain Controller on palvelin, jolla on käynnissä Active Directory Domain Services (Techopedia 2018).

Domain Forest on yleensä useamman domain puun muodostelma. Forestin ylimpänä osuutena toimii domain root, johon voidaan liittää child domaineja. (Microsoft Corporation 2018.)

Sandbox on layer, missä tapahtuu kaikki containerin kirjoitustominnot, kuten tiedostojärjestelmän tai rekisterin muutokset ja sovellusten asennukset (Microsoft Corporation 2016a).

Virtual Machine eli virtuaalikone. Virtuaalikone on ohjelmallisesti simuloitu itsenäinen käyttöjärjestelmä, jota ajetaan esim. VirtualBoxissa. (Wikipedia 2018.)

Windows Nano Server on Windows Server 2016 mukana tullut asennusvaihtoehto, joka on Windows Server Coreakin kevyempi (Microsoft Corporation 2017b).

1 JOHDANTO

Valitessani opinnäytetyötä, tiesin että haluan tehdä sen Windows-palvelinympäristöstä, mutta halusin lisätä aiheeseen jotain uutta ja ajankohtaista, mitä ei ollut vielä juurikaan käsitelty aikaisemmin. Opinnäytetyöohjaajani suositteli minulle Windows Server 2016 mukana tulevaa container-ominaisuutta, joka on aiheena sekä ajankohtainen että mielenkiintoinen. Rajoittavana tekijänä saattaa toimia palvelimen komponenttipuoli, joka ei koostu palvelimelle tarkoitetuista osista.

Tänä päivänä yhä enemmän pyritään vähentämään palvelinlaitteistoa virtualisoimalla tai pilvipalveluilla. Pienorganisaatioiden tai -yritysten sisäisiin tarkoituksiin ei välttämättä kannata luoda massiivista palvelinfarmia, mutta virtualisoimalla esimerkiksi Linux- tai Windows-palvelin, päästään tarvittavaan lopputulokseen. Virtuaalikoneet syövät kuitenkin host-laitteen resursseja, joten isommissa yrityksissä kannattaakin käyttää fyysistä palvelinta, jonka ympärille yrityksen intra rakentuu. Pilvipalveluilla minimoidaan entistäkin enemmän laitteistoa verrattuna virtuaaliseen paikalliseen järjestelmään, jolloin pilven ylläpito on yleensä toisen yrityksen vastuulla.

Pienorganisaatio, jossa jokaista yrityksen intran ominaisuutta varten on luotu oma virtuaalikone, on tehokas tapa vähentää huoltoaikoja, jos yhtä ominaisuutta täytyy huoltaa tai päivittää, lukuun ottamatta tilannetta, jossa itse fyysinen host-laite menee rikki. Ongelmaksi muodostuu todennäköisesti fyysisen host laitteen kuormitus, jota voidaan vähentää hyödyntämällä container-tekniikkaa.

Windowsin Container on käyttöjärjestelmätason virtualisointiominaisuus, jolla voidaan ajaa useampaa itsenäistä käyttöjärjestelmää samanaikaisesti, ilman että tarvitsee luoda kokonaista virtuaalikonetta, hyödyntämällä host laitteen kernel-tasoa, täten vähentäen resurssien tarvetta. Tämä ominaisuus on lainattu Linux-ympäristöstä (LXC Linux containers) ja sitä mainostetaan lähinnä web- ja ohjelmistokehitystarkoituksiin, sillä siinä on tuki Dockerille. (Microsoft Corporation 2016a.)

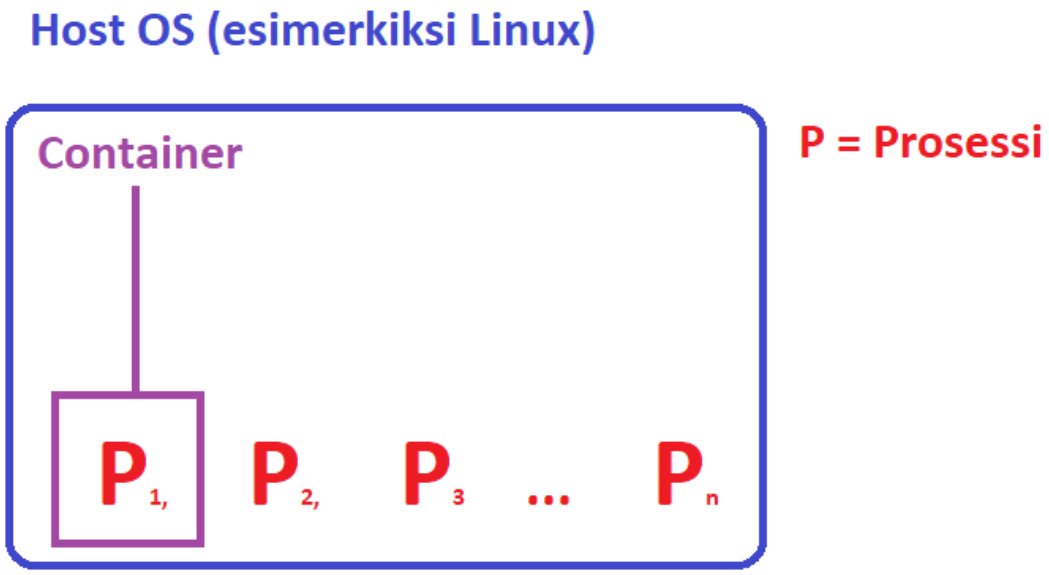
Docker puolestaan on ohjelmistotason virtualisointiohjelmisto, joka pakkaa esimerkiksi web-sovelluksen imageksi. Tämän pitäisi ratkaista ohjelmistokehittäjien ongelma siitä, että ohjelmisto ei toimi jokaisella koneella. (Microsoft Corporation 2016a.)

Container ja docker tarvitsevat kuitenkin jonkinlaisen alustan minkä päällä niitä ajetaan. Tässä työssä käytän, kuten aikaisemminkin mainitsin, tavallista Windows Server 2016, enkä DataCenter-versiota ja testaan Dockerin myös toimintaa Windows 10 puolella. Palvelimelle asennan rooleja ja ominaisuuksia, joita pienorganisaatiossa voisi tarvita (DHCP, DNS, Active Directory). Tämänkaltaisia palvelinympäristöratkaisuja tarvitsee päivä päivältä useampi yritys.

2 TEORIA

2.1 Containerit

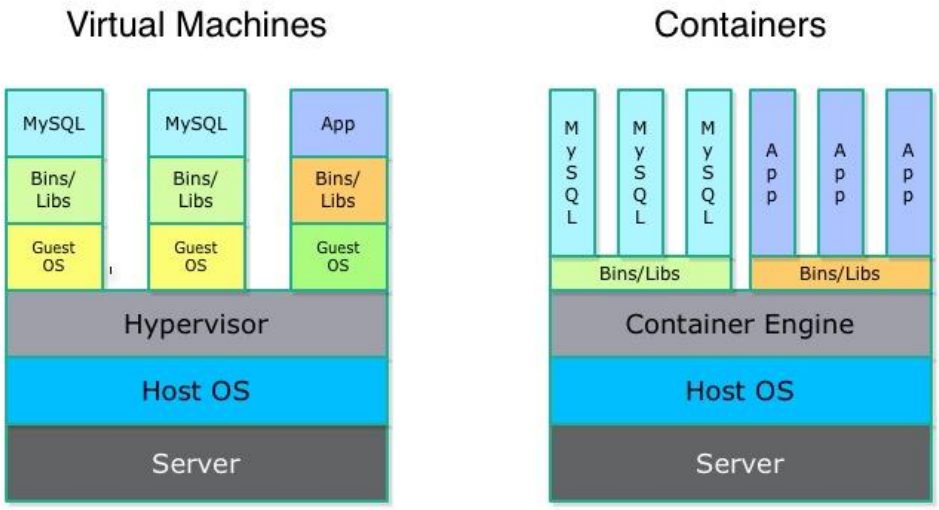
Containereilla tarkoitetaan yleensä yksittäisille prosesseille tarkoitettua ”sandboxia”, jossa ne eristetään host-käyttöjärjestelmästä. Containerin sisällä voidaan ajaa useampaa prosessia, mutta sen tarkoitus on kuitenkin eristää jokin tietty prosessi. Esimerkiksi, jos olisi host käyttöjärjestelmänä Linux-ympäristö, jossa halutaan eristää jokin prosessi, tämä prosessi menee containerin sisälle, jossa se ei vaikuta host käyttöjärjestelmän toimintaan, muuta kuin jakamalla muisti- ja prosessoritehoa. Containerin sisällä prosessilla on oma prosessinimiavaruus (process namespace) ja cgroupit (control groups). (Corrie 2017.) Containerin prosessinimiavaruuden avulla host järjestelmän resursseja voidaan eristää ja virtualisoida ryhmäksi prosesseja (Wikipedia 2017b), kun taas cgroupit rajoittaa containerin resurssien käyttöä (Wikipedia 2017c). Ohessa laatimani kuva havainnollistamaan containerin toimintaa (Kuva 1).



Kuva 1 Prosessin eristäminen containeriin

Tällä periaatteella toimivat nykyisetkin container-alustat (LXC, Windows Server Container, Docker), vaikka käyttötarkoitus ei olisikaan välttämättä pelkän prosessin eristäminen.

Päämäärällisesti virtuaalikone ja container ovat samanlaisia, mutta nimenomaan arkkitehtuuri on näiden ratkaiseva ero, kuten kuvasta (Kuva 2) huomaa. Container-ratkaisusta puuttuu Hypervisor-taso, jota virtuaalikoneet hyödyntävät.



Kuva 2 Virtuaalikoneen ja containerin arkkitehtuurin ero (The Blog of Patrick Galbraith, 2014)

2.1.1 Windows Container

Windows Container on Windows Server 2016 mukana tullut tekniikka, jolla ohjelma saadaan ajettua omassa itsenäisessä säiliössä, jossa sillä ei ole tietoa muista ohjelmista sen ulkopuolella. Microsoftin nettisivujen dokumentaatio vertaa containeria keittiöön, joka on valmiiksi kalustettu. Keittiöön tarvitsee vain liittää sähkö ja vesi, että tämä toimisi, sillä container sisältää valmiin ympäristön tomiakseen. Tällä siis viitataan jaettuun kerneliin. Containerit ovat siis eristettyjä, resursseiltaan rajattuja, liikuteltavia alustoja, joita ajetaan fyysisellä tai virtuaalisella host laitteella. Windows Container on tehokas tapa vähentää kuormaa, jos on tarkoitus eristää Windowsin prosesseja, ominaisuuksia tai rooleja, mutta ei välttämättä haluta useampaa virtuaalipalvelinta tai fyysistä host laitetta. (Microsoft Corporation 2016a.)

On olemassa kahdenlaista Windowsin container-tyyppiä, jotka eroavat vain eristyksen kernel-tasolla:

- Windows Server Containerit toimivat siten, että jakavat kernelin containerin host laitteen ja containereiden välillä. Tämä tekee tästä melko epäturvallisen, jos on tarkoitus ajaa kolmannen osapuolen container imageja. Jaetun kernelin takia containereilla tulee olla sama kernel-versio ja konfigurointi.

- Hyper-V Container on Windows container, jota varten luodaan oma virtuaalikone, joka on eristetty kernel-tasolla Container hostista, tehden tästä turvallisemman.

(Microsoft Corporation 2016b.)

Windows Server Containerin ajaminen onnistuu helposti Windows Nano Serverillä, joka on Windows Server Coreakin kevyempi asennusvaihtoehto Windows Server 2016 -ympäristössä. Nano vie vähemmän asennustilaa, muistia ja on nopeampi käynnistää. Windows Nano Server on tosin rajattu, joten kannattaa tarkistaa, että ohjelman tai palvelun ajaminen on tuettu Nanon ympäristössä. Tästä huolimatta Nano-vaihtoehto on kuitenkin hyvä vaihtoehto container-ympäristöihin, sillä se sisältää vain välttämättömät ominaisuudet palvelimen toiminnalle. Esimerkiksi IIS 10 -tuen lisääminen Nanolle mahdollistaa kevyen, mutta tehokkaan tavan ajaa web-palvelinta containerissa. (Microsoft Corporation 2016c.)

Joka päivä enemmän yleistyvä pilvipalveluteknologia on myös otettu huomioon Microsoftilla, sillä se on pyrkinyt lisäämään Windowsin Container-tekniikan jalansijaa muun muassa Microsoftin Azure-pilvipalvelun avulla. Microsoftilla on näkemys, että lähitulevaisuudessa ainakin osa käyttäjien ohjelmista ajettaisiin pilvessä, mutta toistaiseksi tällä hetkellä Windowsin container-tekniikkaa tukevat Windows Server 2016 ja Azure. (Perlow 2017.)

2.1.2 Docker

Docker on container-ohjelmisto, jonka julkaisi Docker, Inc. maaliskuussa 2013 (Wikipedia 2017d). Se luotiin alun perin nopeuttaakseen yksittäisten LXC-ohjelmien avaamista, luomista, siirtämistä ja kopioimista, ilman että tarvitsee luoda uutta kokonaista virtuaalikonetta. Tämä tapahtui luomalla containerista Docker image, joka on liikuteltava Container tiedosto. Nykyään Docker on oma container-ympäristönsä, joka ei tarvitse Linuxilla LXC:tä toimiakseen, jolla pystytään ajamaan, luomaan ja jakamaan containereita. (Wang 2017.)

Myöskin Windows 10 -käyttöjärjestelmälle on tullut tuki Dockerille. Vaatimuksina on fyysinen host-laite, jonka käyttöjärjestelmänä on Windows 10 Pro, joidenka koontiversion tulee olla vähintään 14393.222 tai uudempi. Myöskin Hyper-V ja Containers ominaisuudet tulee olla päällä (Ohjauspaneeli\Kaikki ohjauspaneelin kohteet\Ohjelmat ja toiminnot → Ota käyttöön Windowsin ominaisuuksia). Suomenkielisessä Windowsissa Containers ominaisuus löytyy nimellä Säiliöt. (Microsoft Corporation 2016d.) Windowsin Dockerilla on myös mahdollista ajaa Linux containereita, tällä tavoin on helppoa esimerkiksi ajaa Linuxin Nginx web-palvelinta (Scherer 2016).

Ohjelmistoa kehittäessä huomataan, että taustalle tarvitaan yleensä tietokanta tai web-service. Tämän takia jokaiselle ominaisuudelle kannattaakin luoda oma containerinsa. Samanaikaisesti useamman containerin luominen onnistuu käyttämällä docker-compose käskyä, joka käyttää YAML-tiedostoa rakentaakseen containerit. (Chance 2016.)

Docker Hub on pilveen perustuva rekisteri palvelu, jonne organisaatio voi luoda oman organisaation tilin. Tilille voidaan linkata omien koodien repositoryt ja lisätä tai ladata itse Docker imageja, joihin käyttäjällä on oikeus. Hubin ominaisuutena on myös automaattinen uuden imagen luominen, kun lähdekoodi repositoryyn tehdään muutoksia. (Docker Inc. 2017.)

2.2 **Active Directory (AD)**

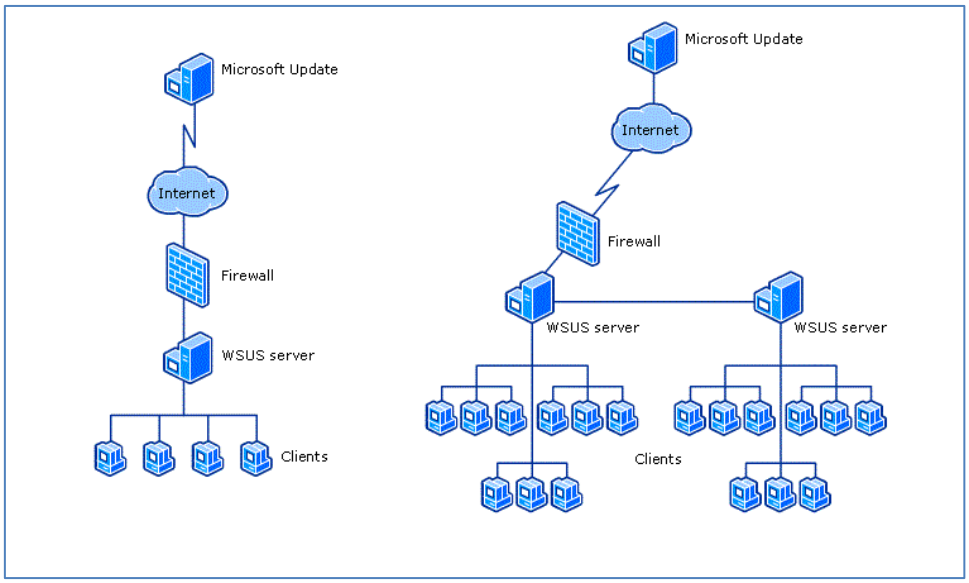
Active Directory mielletään Microsoftin käyttäjätietokantana ja hakemistopalveluna, joka on ollut ominaisuutena Windows Server 2000:sta lähtien (Wikipedia 2017a). Termit Active Directory ja Active Directory Domain Services sekoitetaan helposti, mutta muistisääntönä on se, että AD on joukko palvelinrooleja ja ominaisuuksia, joita voidaan hyödyntää toimialueella, kun taas AD DS on yksi näistä ominaisuuksista (Microsoft Corporation 2013). Kannattaa muistaa, että domain aluetta kutsutaan termillä forest, jossa forest koostuu domaineista. Termi kannattaa muistaa myös syystä, että AD DS -asennusvaiheessa mainitaan useasti forest, eikä välttämättä domain. AD-palveluita löytyy myös muilta valmistajilta ja Microsoftin AD palveluun voidaan liittää myös Linux- ja Mac-koneita. (Eli the Computer Guy 2013a.)

Lähes jokaisella pienorganisaatiolla on käytössä Active Directory, sillä sen avulla saadaan toimialueen sisällä paikallinen järjestelmänvalvoja voi vaivattomasti lisätä ja poistaa uusia käyttäjätilejä ja tietokoneita Domain Controller -koneella (DC). Muutokset AD:lle tulevat voimaan kaikkiin koneisiin, jotka on liitetty organisaation toimialueelle. Domain Controllerilla voidaan myös määritellä Active Directoryyn ryhmiä. Esimerkiksi jos organisaatio tarvitsee vaikkapa johtoportaalle, kirjanpidolle tai muulle ryhmälle omat oikeutensa tiettyihin ohjelmiin, kansioihin tai ominaisuuksiin, sen voi tehdä AD DS:llä tekemällä muutoksia Group Policyihin. Näitä ryhmiä kutsutaan usein nimellä Organizational Unit (OU). (Eli the Computer Guy 2013a.)

Esimerkiksi ammattikorkeakoulussa, jossa on toimipisteitä eri puolilla maakuntaa, voidaan jokaiselle toimipisteelle määrittää paikallinen järjestelmänvalvoja, joka on vastuussa kyseisen pisteen toiminnasta. Tällä järjestelmänvalvojalla on oikeus vain kyseisen toimipisteen laitteisiin ja käyttäjiin, mutta ei muiden toimipisteiden.
Active Directory Domain Controllereita voidaan myös luoda useampia, jotka keskustelevat keskenään. Microsoft itse suosittelee heidän Technet-dokumentaatiossa, että Active Directory -järjestelmässä olisi ainakin kaksi Domain Controlleria, jotta järjestelmä olisi mahdollisimman varma. (Microsoft Corporation 2009.) Tällä tavoin voidaan jakaa kuormaa tasaisesti tai luoda fallback DC, jos ensisijainen DC menee epäkuntoon.

2.3 WSUS

Windows Server Update Services (WSUS) on Windows-palvelimelle asennettava rooli, jolla voidaan hallinnoida toimialueen client-laitteille ladattavia päivityksiä. Tällä tavoin järjestelmänvalvoja pystyy hallitsemaan mitä päivityksiä ja milloin ne asennetaan client-laitteille, joka on yrityksille olennaista. (Microsoft Corporation 2017c.) Yrityksellä saattaa olla käytössä CRM-ohjelmisto tai muita oman liiketoiminnan kannalta tärkeitä ohjelmia, joiden toimintaa tietyt Windows-päivitykset saattavat häiritä. Esimerkiksi suuremmat päivitykset, kuten Windows 10 Anniversary Update (koontiversio 1607), jonka myötä monen ihmisen tietokone meni tavalla tai toisella epäkuntoon. (Leonhard 2016.) Näiden koontiversiopäivitysten asentaminen kaikille yrityksen koneille on melkoinen riski, jos niitä ei asenneta hallitusti ja aikataulutetusti. Toinen ongelma koontiversiopäivityksissä on niiden asentamisen hitaus, sillä ne ovat tunnettuja monen tunnin asennusajasta. Päivitystenhallintaa varten voidaan luoda Group Policy -ryhmiä, joiden mukaan päivitykset asentuvat, jotta päivitykset eivät asennu samaan aikaan tai kaikille koneille. WSUS-palvelimia voi olla myös useampikin yrityksen sisällä, jolla voidaan jakaa kuormaa tai määrittää tietyt laitteet hakemaan päivityksensä toiselta WSUS-palvelimelta.



Kuva 3 WSUS Deployment Scenarios (Microsoft Texchnet, n.d.)

2.4 DHCP

Dynamic Host Configuration Protocol (DHCP) on yksinkertaisimmillaan IP-osoitteen automaatista määrittämistä esimerkiksi reitittimeltä. Tämän voi kuitenkin lisätä erilliseksi rooliksi Windows Serverille. Tämä edellyttää sitä, että reitittimeltä on otettu DHCP pois päältä, ja DHCP-rooli on lisätty Windows palvelimelle. DHCP on hyvä lisätä palvelimelle, sillä se vähentää manuaalista työskentelyä ja mahdollisia IP-osoite päällekkäisyyksiä. Joissakin tilanteissa DHCP-palvelimen ja client-laitteen välissä saattaa olla palvelin. Tässä tilanteessa olisi järkevää asettaa välissä oleva palvelin toimimaan DHCP Relay Agenttina. DHCP Relay Agent välittää client-laitteen DHCP-pyynnön DHCP-palvelimelle ja välittää IP-osoite-ehdotuksen DHCP-palvelimelta client-laitteelle, jonka client sitten hyväksyy (Eli the Computer Guy 2013b.)

2.5 **DNS**

Järjestelmänvalvojan tehtäviä voi huomattavasti helpottaa DHCP:n ja AD:n ohella Domain Name System eli DNS. IP-osoitteiden muistaminen ei ole kaikille helppoa, varsinkin jos organisaatiossa on vaihtuva IP-osoite tai useampi järjestelmänvalvoja. Domain Name Systemin avulla IP-osoite muunnetaan haluamaksi merkkijonoksi. DNS on mahdolista asentaa Active Directory Directory Servicen asennuksen yhteydessä. Esimerkiksi organisaatiossa, jossa järjestelmänvalvoja haluaa yksinkertaistaa staattisten IP-osoitteiden omaavien laitteiden lisäämistä, voi hän asettaa tulostinten tai muiden verkkolaitteiden IP-osoitteiden kohdalle palvelimen DNS:n asetuksissa esimerkiksi ”PRINTER1”. Dynaamisia IP-osoitteita varten tulisi määrittää DDNS, eli Dynamic DNS (Eli the Computer Guy 2013c.)

3 **LAITTEISTO**

Laitteistona on käytössä palvelimena vanha pöytäkoneeni, joka koostuu seuraavista:

- AMD FX-6300 CPU
- 8 gigatavua DDR3 muistia
- 500 gigatavun mekaaninen kiintolevy
- 240 gigatavun SSD-kiintolevy
- AMD R9 Nano.

Palvelimen osat eivät ole tarkoitettu palvelinkäyttöön, mutta riittävät tämän opinnäytetyön tarkoituksiin.

Verkkopuoli hoidetaan Huawein CPE B593 4G-reitittimellä, jolta otetaan DHCP pois käytöstä, jotta Windows Serverin DHCP:n kanssa ei synny ristiriitoja.

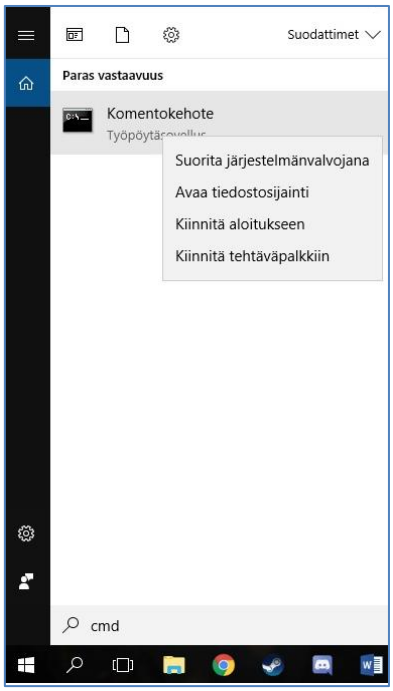
Client-laitteena toimii pöytäkoneeni, jolta löytyy Windows 10 Pro -käyttöjärjestelmä, jotta laite saadaan liitettyä Domainiin.

4 **PALVELIMEN ASENNUS**

Ympäristön luominen aloitetaan asentamalla Windows Server 2016 -palvelimelle USB-tikun avulla. Lisenssin ja käyttöjärjestelmä saatiin Microsoftin Dreamspark-palvelusta, käyttäen koulun tunnuksia. Tämän lisenssin käyttö on rajattu vain omaan käyttöön, eikä kaupalliseen. Ladataan .ISO-tiedoston linkistä, joka löytyy Dreamsparkista ja avataan tiedosto esimerkiksi Daemon Tools-ohjelmalla.

4.1 **Asennusmedian luominen**

Kun .ISO-tiedosto on ladattu, mountataan se Daemon TOOLSilla. Tämän jälkeen asetetaan USB-tikku koneeseen ja avataan komentokehto järjestelmänvalvoja oikeuksilla. (Kuva 4)



Kuva 4 Komentokehote järjestelmänvalvojana

Komentokehotteessa ajetaan seuraavat komennot:

diskpart Tällä avataan diskpart työkalu, jolla valmistellaan muistitikku.

list disk Tällä listataan kaikki koneeseen liitetyt kiintolevyt ja etsitään listasta muistitikku. Tässä tapauksessa se on Disk 3, sillä muistitikun koko on 29 gigatavua. (Kuva 5)

```
C:\WINDOWS\system32>diskpart

Microsoft DiskPart version 10.0.16299.15

Copyright (C) Microsoft Corporation.
On computer: DESKTOP-QJPA5U5

DISKPART> list disk

  Disk ###  Status         Size     Free     Dyn  Gpt
  --------  -------------  -------  -------  ---  ---
  Disk 0    Online          931 GB      0 B
  Disk 1    Online          223 GB      0 B        *
  Disk 2    Online          232 GB      0 B        *
  Disk 3    Online           29 GB      0 B

DISKPART>
```

Kuva 5 Luettelo kiintolevyistä

sel disk 3 Valitaan USB-muistitikku (Kuva 6).

clean Tämä tyhjentää valitun levyn partitioista (Kuva 6).

create partition primary Luodaan Primary partitio muistitikulle, jolta bootataan asennusmedia (Kuva 6).

```
DISKPART> sel disk 3

Disk 3 is now the selected disk.

DISKPART> clean

DiskPart succeeded in cleaning the disk.

DISKPART> list disk

  Disk ###  Status         Size     Free     Dyn  Gpt
  --------  -------------  -------  -------  ---  ---
  Disk 0    Online          931 GB      0 B
  Disk 1    Online          223 GB      0 B        *
  Disk 2    Online          232 GB      0 B        *
* Disk 3    Online           29 GB    29 GB

DISKPART> create partition primary

DiskPart succeeded in creating the specified partition.
```

Kuva 6 Partitiointi

sel partition 1 Valitaan Primary partition. Oletuksena tämä pitäisi olla jo valittuna (Kuva 7).

active Merkitään Primary partition aktiiviseksi (Kuva 7).

format fs=exfat Formatoidaan muistitikku ja vaihdetaan tiedostojärjestelmäksi, sillä tiedostokoko on melko suuri, sekä nimetään uudelleen (Kuva 7).

```
DISKPART> list partition

  Partition ###  Type              Size     Offset
  -------------  ----------------  -------  -------
* Partition 1    Primary             29 GB  1024 KB

DISKPART> sel partition 1

Partition 1 is now the selected partition.

DISKPART> active

DiskPart marked the current partition as active.

DISKPART> format fs=exfat quick label="win2016"

  100 percent completed

DiskPart successfully formatted the volume.
```

Kuva 7 Formatointi

Tämän jälkeen poistutaan diskpartista komennolla exit.
Tämän jälkeen katsotaan resurssienhallinnasta, minkä kirjaimen Daemon TOOLS on määrittänyt mountatulle .ISO-tiedostolle. Tässä tapauksessa ”I”. Seuraavilla komennoilla kopioidaan asennusmedian tikulle:

i: Siirrytään I-asemalle (Kuva 8).

cd boot Siirrytään asennusmedian boot-hakemistoon (Kuva 8).

bootsect /nt60 g: Päivittää master boot coden BOOTMGR:n ja NTLDR:n välillä (Kuva 8).

xcopy i:*.* g:\ /E /H /F Tämä kopioi kaiken I-asemalta H-asemalle. E-parametri kopioi tyhjät hakemistot, H-parametri kopioi piilotetut hakemistot ja F-parametri näyttää ajaessa mitä kopioidaan. Tämä vaihe kestää jonkin aikaa, joten kannattaa olla kärsivällinen (Kuva 8).

```
DISKPART> exit

Leaving DiskPart...

C:\WINDOWS\system32>i:

I:\>cd boot

I:\boot>bootsect /nt60 g:
Target volumes will be updated with BOOTMGR compatible bootcode.

G: (\\?\Volume{07d159f8-803c-11e7-888e-806e6f6e6963})

    Successfully updated exFAT filesystem bootcode.

Bootcode was successfully updated on all targeted volumes.

I:\boot>xcopy i:\*.* g:\ /E /H /F
```

Kuva 8 Asennusmedian kopioiminen

Tämän jälkeen asennusmedia on valmis ja täytyy vain bootata palvelimella asennusta varten. Tässä vaiheessa ainoa huomioitava asia on, haluaako graafisen käyttöliittymän palvelimelle (Desktop Experience), muuta erikoista tässä vaiheessa ei ole. Voidaan valita graafinen käyttöliittymä, sillä se helpottaa käyttöä huomattavasti.

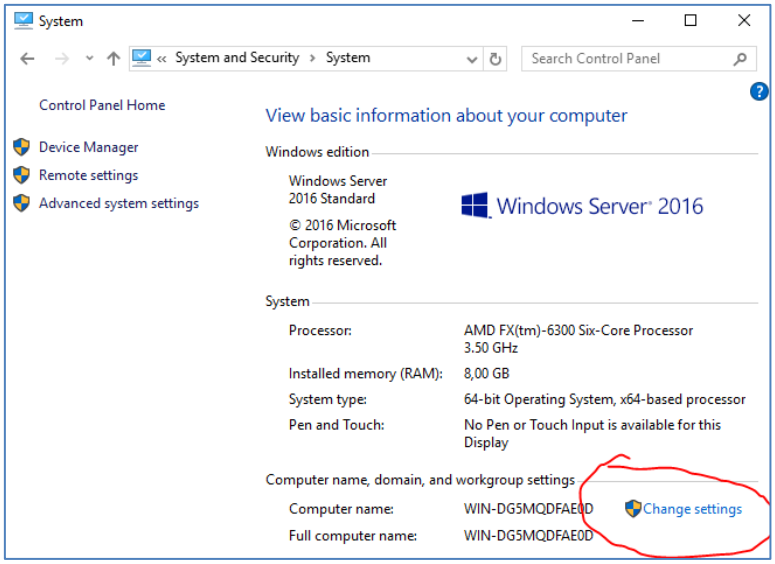
4.2 Palvelimen käyttöönotto

Asennuksen päätteeksi kysytään käyttäjältä, mikä tulee järjestelmänvalvojan salasanaksi. Tämä salasana kannattaa mahdollisesti jopa dokumentoida, jos on pienikin epäilys, että sen voi unohtaa tai käytössä on epämääräinen merkkijono. Tämän jälkeen kirjaudun sisään palvelimelle ja aluksi kannattaa tarkistaa ajurit ja päivitykset, sillä tietoturvapäivitykset ovat tärkeitä. Käytössä olevat osat eivät ole suoranaisesti suunniteltu palvelinkäyttöön, joten osa ajureista voi olla Windows 10 -ajureita, sillä Windows Server 2016 perustuu samaan pohjaan. Myös Windows Server 2012:n kanssa pystyttiin ajamaan Windows 8:lle tarkoitettuja ajureita samaisesta syystä. Tämä ei kuitenkaan takaa täyttä varmuutta ajureiden toiminnalle. Tavallisessa käytössä palvelin ei todennäköisesti tarvitse erillistä näytönohjainta vaan käyttää integroitua grafiikkapiiriä, mutta voi tulla vastaan tilanteita, joissa tämä ei päde. Esimerkiksi AMD:n ensimmäisen sukupolven Ryzen-prosessoreista ei löydy integroitua näytönohjainta, joka kannattaa pitää mielessä, jos aiotaan käyttää kyseistä prosessorimallistoa palvelimella. Integroitu näytönohjain on kuitenkin täysin oikeutettu valinta, jos palvelimen tarkoituksena ei ole graafinen laskenta.

Asennetaan R9 Nanon uusimmat ajurit, jotka ovat tarkoitettu 64-bittiselle Windows 10:lle, joka toimii moitteettomasti. Tämä vahvistaa käsitystä, että Windows Server 2016 ei aina tarvitse sille suunnattuja ajureita.

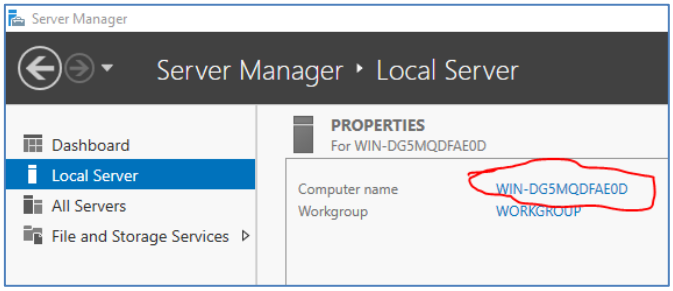
On myös kannattavaa vaihtaa palvelimen nimi, sillä oletuksena palvelimen nimeksi tulee jonkinlainen epämääräinen merkkijono. Tämä auttaa laitteiden tunnistamisessa, jos ympäristössä on useampi palvelin tai palvelimelle yhdistäessä etäältä. Helposti muistettava nimi voisi olla esimerkiksi ”SERVER”. Palvelimen nimen muutos tapahtuu siirtymällä seuraavasti:

Control Panel → System and Security → System → Change settings (Kuva 9)



Kuva 9 Nimen vaihtaminen ohjauspaneelissa

Tai Server Managerissa Local Server-osiossa (Kuva 10).



Kuva 10 Nimen vaihtaminen Server Managerissa

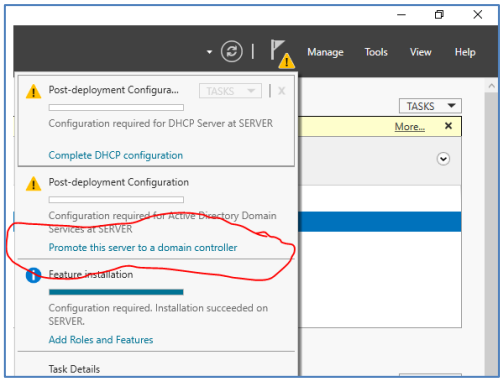
Tämän jälkeen palvelin käynnistetään uudelleen ja voidaan ruveta asentamaan palvelimelle tarvittavia rooleja ja ominaisuuksia.

4.3 **Active Directory Domain Services, DHCP ja DNS**

Windows Serverissä on helppokäyttöinen Add Roles and Features Wizard-ohjelma, jolla on helppo asentaa tarvittavat ominaisuudet palvelimelle. Kaikki tämän vaiheen roolit voidaan asentaa helposti samaan aikaan, kun Server Managerin Dashboardilla siirrytään ”Add roles and features”-osioon tai Server Managerin ”Manage”-osiossa ja valitaan ”Add roles and features”.

Tämän jälkeen valitaan asennustyypiksi rooli- tai ominaisuuspohjainen asennus, joka on oletuksenakin. Tämän jälkeen on valittavissa, mille palvelimelle asennetaan rooleja tai ominaisuuksia, joka on tässä tapauksessa helppoa, sillä on vain yksi palvelin käytettävissä, jonka nimi on ”SERVER” nimenmuutoksen jälkeen. Server roles-listasta valitaan seuraavaksi Active Directory Domain Services, DHCP ja DNS. Jokaisella valinnalla aukeaa ikkuna, joka kertoo mitä roolit tarvitsevat toimiakseen, jotka asentuvat, kun valitsee Add Features. Roolien asentamiseen palataan myöhemmin Container-vaiheessa. Tämän jälkeen asennus kertoo asennettavista rooleista, joita käydään teoria-osuudessa lävitse, mutta tärkeänä huomiona kannattaa nyt viimeistään olla reitittimen oma DHCP pois päältä. Lopuksi valitaan ”Install”, jonka jälkeen ominaisuuksia asennetaan. Tässä vaiheessa voi kulua jopa puoli tuntia, jonka jälkeen Server Manageriin ilmestyy lisää vaihtoehtoja.

Aloitetaan Active Directory Directory Servicesista, joka löytyy vasemmalta listasta. Palvelimesta tehdään Domain Controller, jotta saadaan Domain luotua. Tämä tapahtuu valitsemalla ”Promote this server to a domain controller”-vaihtoehdolla (Kuva 11).



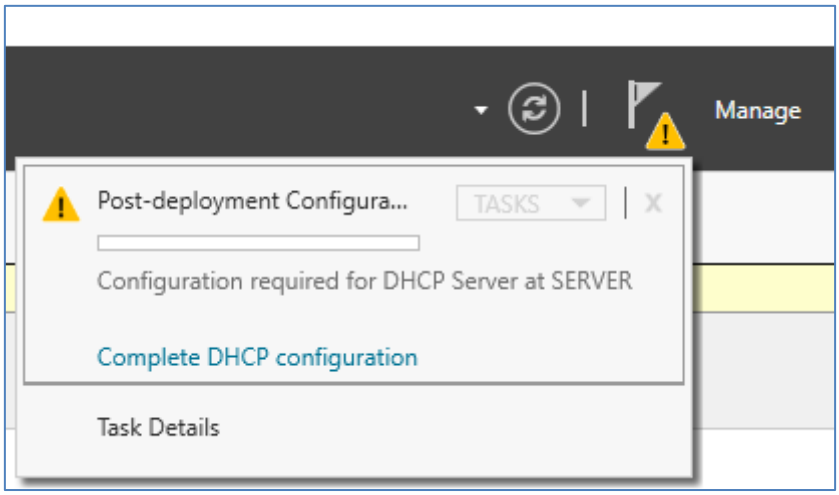
Kuva 11 Promote to a domain controller

Tällä avataan AD DS Configuration Wizard, jonka avulla voidaan luoda domain forest, liittää forestiin uusi DC tai luoda uusi domain forestiin. Valitaan ”Add a new forest”, jolla luodaan uusi toimialue ja valitaan root domain name. Testiympäristössä ei tarvitse omistaa domainia, sillä se toimii vain sisäverkossa. Root domain name haetaan sisäverkon DC palvelimelta, jonka vuoksi esimerkiksi ”organsaatio.fi”-tyyliset sivut kannattaa unohtaa, sillä client-laitteet eivät pääse selaimessa samannimisille sivuille. Vaihtoehto olisi esimerkiksi ”.local”-päätteinen toimialue, mutta tästä on ristiriitaa IT-alalla, onko ”.local”-päätteinen järkevä ratkaisu (Marra 2012). Vaihtoehtoisena turvallisena ratkaisuna olisi esimerkiksi ”ad.organisaatio.fi”. Siinä tapauksessa, jos halutaan web-palvelin taustalle, kannattaa ennalta tarkistaa onko ”organisaatio.fi” domain varattu, jos yrityksen web-sivustoon on tarkoitus päästä ulkoverkosta. ”Read only domain controller (RODC)” -vaihtoehto kannattaa jättää väliin tässä tapauksessa, sillä ympäristöön luodaan vain yksi domain controller.

Kirjoitetaan haluttu salasana DSRM-moduulia varten ja valitaan ”Seuraava”. DNS-asetukset voidaan toistaiseksi jättää huomioimatta ja valitaan ”Seuraava”. NetBIOS-kohdassa voidaan vaihtaa ehdotuksen tilalle esimerkiksi ”ORGANISAATIO”. ”Paths”-osioon ei tarvitse tehdä tällä hetkellä muutoksia ja ”Review Options”-osio näyttää aiemmin tehdyt valinnat, joten valitaan ”Seuraava”. ”Prerequisites Check” -osio varmistaa, että palvelin on valmiina AD:ta varten. Punainen error-ilmoitus tässä vaiheessa voi johtua esimerkiksi, että palvelin ei ole yhteydessä verkkoon, joka korjataan nopeasti liittämällä palvelin verkkoon. Muista varoituksista ei kannata välittää tässä vaiheessa ja valitaan ”Install”. AD-asennuksen jälkeen palvelin käynnistyy uudelleen, jonka jälkeen tulee kirjautumisruutu, jossa huomataan NetBIOS-nimen ilmestyneen käyttäjänimen edelle. Tämä tarkoittaa, että domain on luotu ja AD:lle voidaan ruveta syöttämään käyttäjiä ja tietokoneita.

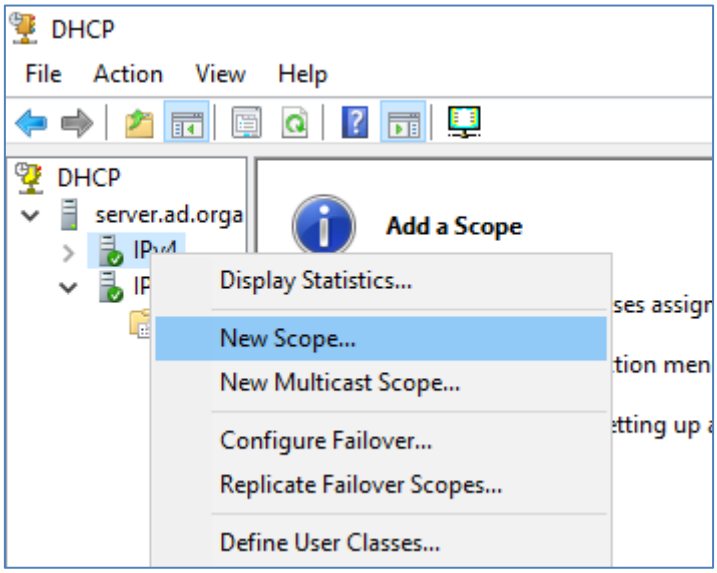
Tässä välissä asennetaan kuitenkin DHCP ja palataan AD-osioon myöhemmin. Varmistetaan, että DHCP-ominaisuus on otettu pois käytöstä reitittimen päästä ottamalla selaimen kautta yhteys reitittimeen. Vanhemmissa laitteissa ei välttämättä ole selainpohjaista graafista käyttöliittymää, vaan terminaalimallinen komentorivi, mutta lähes kaikki uudemmat laitteet ovat selaimella hallittavia.

Tämän jälkeen siirrytään Windows-palvelimen Server Managerissa DHCP Configuration -vaiheeseen (Kuva 12).



Kuva 12 DHCP-konfiguraatio

DHCP roolin myötä Domainiin liittyneet Client-laitteet hakevat IP-osoitteensa Windows Serverin omalta DHCP:lta. Roolin käyttöönotto on nopea, sillä ”Authorization”-kohdassa on defaultina oikea vaihtoehto. Tässä välissä palvelin käynnistetään uudelleen, jonka jälkeen tehdään konfiguraatiot DHCP:lle Server Managerin ”Tools”-välilehden ”DHCP”-osiossa. Tämän pitäisi avata DHCP-hallintapaneelin, jossa lisätään uusi IPv4:ä käyttävä DHCP Scope, johon määritetään jaettavat ja pois jätetyt IP-osoitteet (Kuva 13).

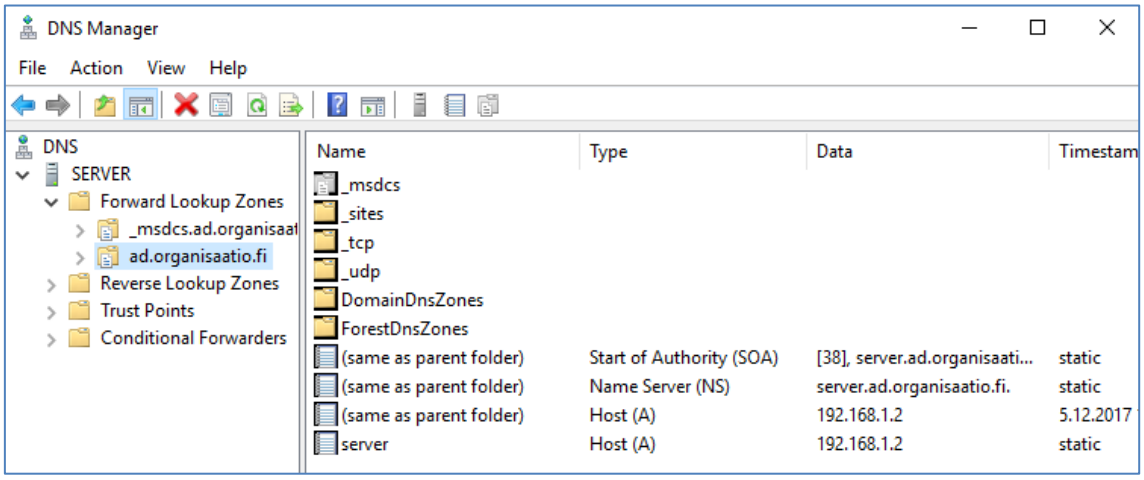


Kuva 13 DHCP IPv4 Scopen konfigurointi

DHCP-asennuksessa kirjoitetaan ensiksi nimi DHCP Scopelle, joka auttaa erottelemaan eri aliverkkojen Scopet. ”Description”-kentän voi jättää tyhjäksi, jonka jälkeen asetetaan DHCP Poolin ensimmäinen ja viimeinen IP-osoite, jättäen pois host- ja broadcast-osoitteet (192.168.1.0 ja 192.168.1.255), esimerkiksi 192.168.1.1 – 192.168.1.254, josta voi jättää seuraavassa vaiheessa pois tarvittava määrä kiinteitä osoitteita esimerkiksi tulostimia, hallittavia kytkimiä tai palvelimia varten. Valitaan esimerkiksi ensimmäiset 30 mahdollista IP-osoitetta 192.168.1.1 – 192.168.1.30 pois poolista, niin riittää varmasti staattiset osoitteet, eikä tulisi IP-osoite konflikteja. Tämän jälkeen kysytään käyttäjältä

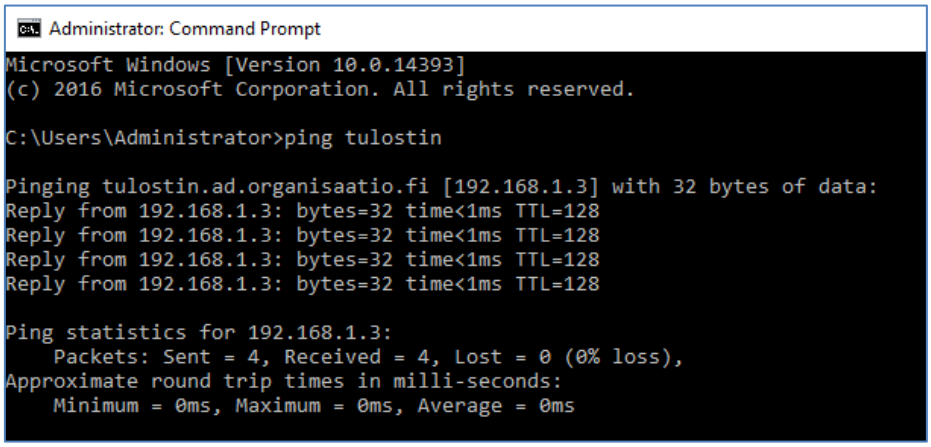
Lease-aikaa, joka defaultina on 8 päivää, jonka pitäisi olla riittävä. Seuraavaksi voidaan konfiguroida DHCP Scopen asetukset. Seuraavaksi määritetään DHCP:n clienteille käytettävä reitittimen IP-osoite (192.168.1.1) ja DNS-palvelimeksi Windows-palvelimen IP-osoite (192.168.1.2). WINS osio voidaan sivuuttaa, sillä se ei ole niin olennainen tänä päivänä, kun DNS on olemassa. Tämän jälkeen otetaan DHCP Scope käyttöön.

Siirrytään tarkastelemaan DNS-asetuksia Server Managerissa ”Tools”-osiossa, jossa valitaan ”DNS”. Tämä avaa DNS Managerin, jossa voidaan lisätä verkon laitteille, joilla on staattinen IP-osoite, jonkinlainen nimi, jolla voidaan yhdistää laitteeseen ilman IP-osoitetta. Vakiona listasta löytyy Windows-palvelin, joka tässä tapauksessa näkyy listassa nimellä ”server” ja IP-osoite on 192.168.1.2 (Kuva 14).



Kuva 14 Kuvakaappaus DNS Managerin Forward Lookup Zones -listasta

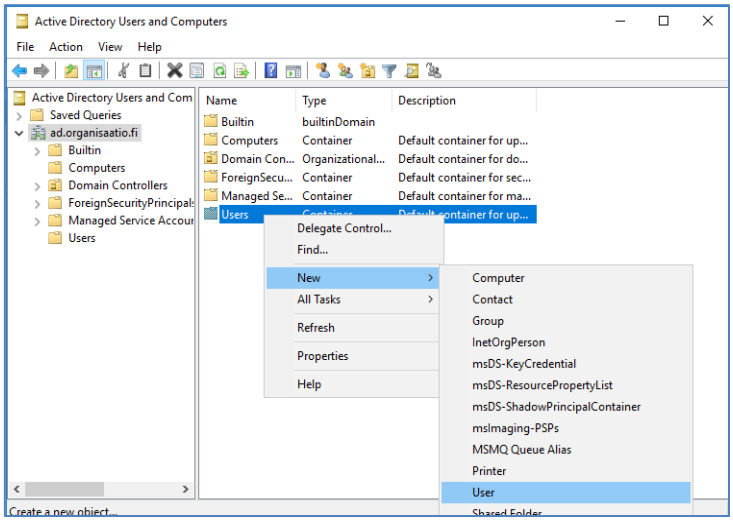
Listaan voidaan lisätä verkkotulostin, jolle on määritetty IP-osoite 192.168.1.3, jolle voidaan DNS:n avulla kiinnittää nimi ”tulostin”. Tämä määritetään valitsemalla ”New Host (A or AAAA)” vaihtoehdolla ja määrittämällä tulostimelle nimi (tulostin) ja tulostimen staattinen IP-osoite (192.168.1.3). Tämän jälkeen listassa tulisi olla ”serverin” lisäksi ”tulostin”, jonka toimivuus voidaan varmistaa, ajamalla komento ”ping tulostin” komentokehotteessa (Kuva 15). Tällä tavoin voidaan tarvittaessa kiinnittää staattisille IP-osoitteille nimiä. Verkossa ei oikeasti ole tulostinta, vaan tavallinen pöytäkone, jolle on määritetty kiinteä IP-osoite, mutta samalla käytännöllä toimii tulostimen IP-osoitteen nimeäminen.



Kuva 15 Merkkijonoksi muutetun IP-osoitteen pingaaminen

4.4 Active Directoryn hallinta

Tässä vaiheessa ryhdytään lisäämään käyttäjätilejä Active Directoryyn, joita voidaan käyttää client-laitteilla. Näitä voidaan lisätä Server Managerin ”Tools”-osion ”Active Directory Users and Computers” paneelissa. Listasta pitäisi löytyä luotu domain, joka tässä tapauksessa on ”ad.organisaatio.fi”, jonka ”Users” hakemistoon lisätään uusi käyttäjä (Kuva 16).



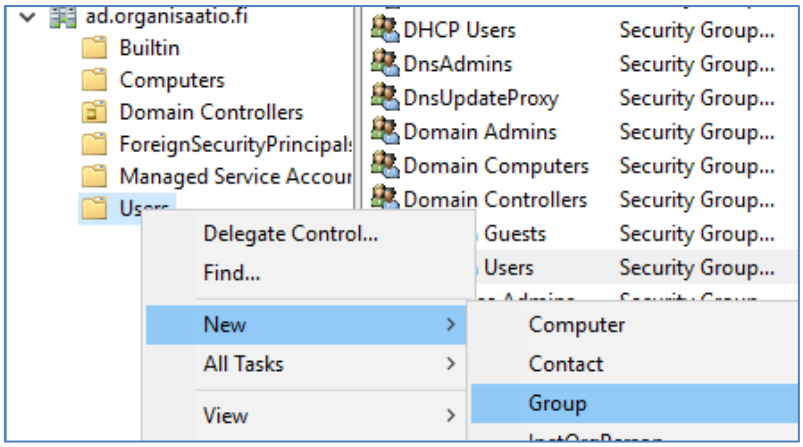
Kuva 16 Lisää käyttäjä Active Directoryyn

Uudelle käyttäjälle määritetään etunimi, sukunimi, kirjautumisnimi ja mihin domainiin käyttäjä luodaan, jonka jälkeen voidaan luoda salasana. Tilille voidaan määrittää tässä vaiheessa seuraavia lisävalintoja:

- Pakotettu salasanan vaihto käyttäjän kirjautuessa ensimmäistä kertaa koneelle
- Käyttäjä ei voi vaihtaa salasanaa
- Salasana ei koskaan vanhene
- Tili on pois käytöstä.

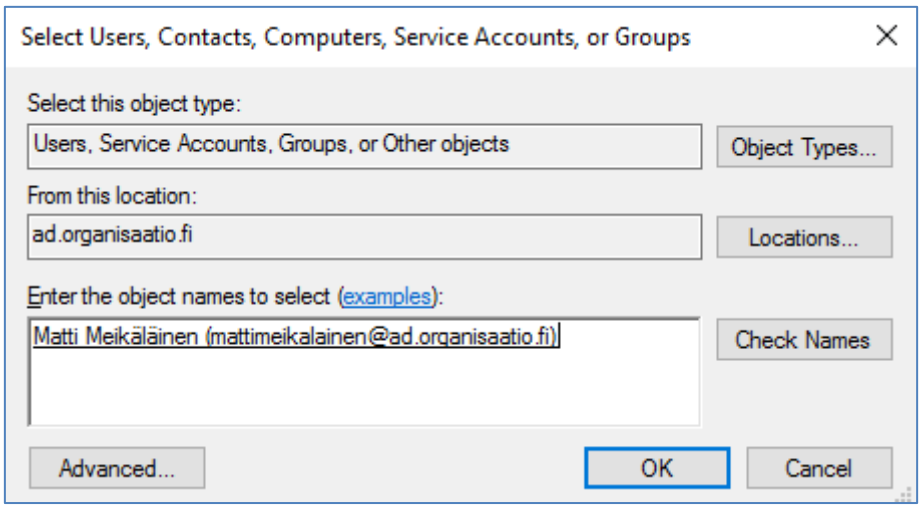
Nämä kaikki vaihtoehdot ja paljon muuta voidaan tosin myöhemminkin määrittää käyttäjälle, joten voidaan jättää kaikki vaihtoehdot pois. Kirjoitetaan haluttu salasana, jonka tulee oletuksena täyttää tarvittavat kriteerit eli kolme erilaista merkkiä (iso kirjain, pieni kirjain, numero, aakkos- tai epäaakkosnumeerinen merkki). Tämän jälkeen käyttäjän tiedot näytetään ja valitaan ”Finish”. Käyttäjä on luotu ja se lisätään automaattisesti Domain Users -ryhmään. Tällä käyttäjällä voidaan nyt kirjautua domainiin liitetyllä client-laitteella. AD Users and Computers paneelin Domainin Users-hakemistossa voidaan myös muokata käyttäjän oikeuksia valitsemalla käyttäjän kohdalla ”Properties” ja menemällä ”Account”-välilehteen, mutta Group Policyiden avulla voidaan muokata samaan aikaan useamman käyttäjän oikeuksia määrittämällä ryhmälle erilaisia oikeuksia ja siirtämällä käyttäjiä haluttuun ryhmään. Tämä auttaa etenkin isommissa organisaatioissa.

Ryhmän luominen tapahtuu melko samanlailla, kuin käyttäjän luominen, mutta määritysvaihe on nopeampi (Kuva 17). Luodaan ryhmä ”test group”, johon lisätään aiemmin luotu testikäyttäjä ”mattimeikalainen”. Group scopena pidetään oletus ”Global” ja Group type pysyy oletuksessa ”Security”, sillä tämänkaltaisessa pienessä palvelinympäristössä ei tarvitse miettiä domainien välisiä käyttäjätilejä tai ryhmiä.



Kuva 17 Ryhmän luominen

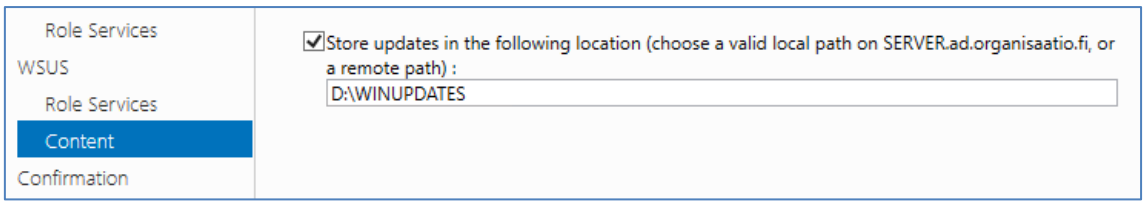
Käyttäjä lisätään luotuun ryhmään valitsemalla test groupin Propertiesissa ”Members”-välilehdessä ”Add…”. Tämä avaa ikkunan jonka tekstikenttään kirjoitetaan halutun käyttäjän käyttäjänimi tai ainakin osa siitä. Kirjoitetaan esimerkiksi ”matti” ja valitaan ”Check Names”, palauttaa domainin käyttäjistä ne, joiden käyttäjänimi sisältää merkkijonon ”matti”. Valitaan ”Ok”, jonka jälkeen käyttäjä ”mattimeikalainen” on luodun ryhmän jäsen. (Kuva 18).



Kuva 18 Käyttäjän lisääminen ryhmään

4.5 Windows Server Update Servicesin asennus

WSUS asentuu Add Roles and Features -ohjelman avulla, josta asennetaan Windows Server Update Services ja sen tarvitsemat ominaisuudet. WSUS-roolin asennus on melko suoraviivainen prosessi, mutta viimeisessä kohdassa voidaan määritellä polku, minne päivitykset tallentuvat. (Kuva 19)



Kuva 19 WSUS-päivitysten polku

Asennuksen päätteeksi kannattaa käynnistää palvelin uudestaan, että ominaisuudet saadaan otettua käyttöön. Tämän jälkeen kannattaa tarkistaa, että mahdollinen palomuuri ei estä yhteyttä palvelimen ja client-laitteiden välillä ja, että yhteys WSUS-palvelimen ja Windows Update -palvelimen välillä toimii. Seuraavaksi siirrytään WSUS Configuration Wizardiin siirtymällä Server Managerissa ”Tools → Windows Server Update Services”.

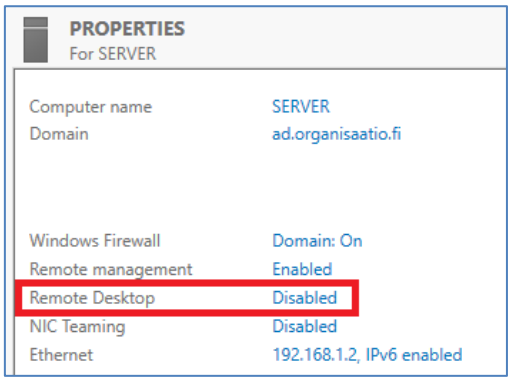
Ensimmäisellä käynnistyksellä WSUS avaa WSUS Configuration Wizardin, jolla voidaan nopeasti määrittää palvelin kuntoon. Tässä tapauksessa ei tarvitse asetuksia muuttaa juurikaan, sillä käytössä ei ole erillistä palomuuria tai useampaa WSUS palvelinta. Vasta ”Specify Proxy Server” -kohdassa tarvitsee valita ”Start Connecting”, joka tallentaa ja lataa päivityspalvelimen tiedot. Tässä vaiheessa kestää luultavasti useampi minuutti.

Tämän jälkeen voidaan valita millä kielellä päivityksiä haetaan. Tässä tapauksessa voidaan valita pelkästään kieliksi suomi, ruotsi ja englanti, jonka jälkeen valitaan ohjelmat, jotka päivitetään WSUS:n kautta. Oletuksena WSUS lataa vain Windows-päivitykset, mutta valitaan vielä esimerkiksi Office-päivitykset, sillä ne ovat olennainen osa lähes jokaisen yrityksen arkea. Tämän jälkeen voidaan valita, minkälaisia päivityksiä WSUS lataa. Tähän kohtaan voidaan vain valita ”Next”, sillä tässä työssä ei keskitytä niin tarkasti WSUS-palvelimiin, vaan pääpiirteittäin.

Sync Schedulessa voidaan määrittää, kuinka monta kertaa palvelin hakee päivityksiä ja monelta haku alkaa. Voidaan valita ”Next” ja laitetaan rasti ”Begin initial synchronization” kohtaan ja valitaan ”Finish”. Tämän jälkeen tarvitsee vielä määrittää WSUS:ta käyttävät laitteet. WSUS hallintapaneelissa voidaan lisätä laitteet käyttämään WSUS:ta. Luodaan uusi tietokoneryhmä esimerkiksi ”Testiryhmä”, jonne lisätään CLIENT1 tietokone.

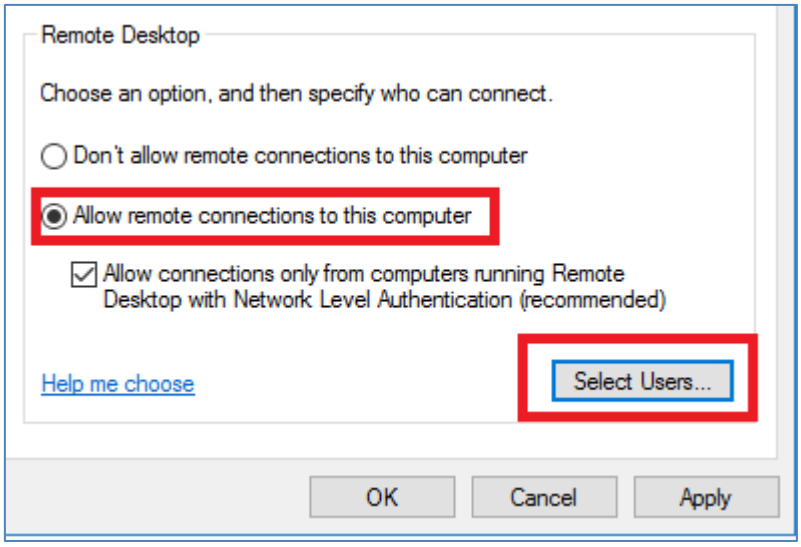
4.6 **Etähallinta**

Järjestelmänvalvojan työtä helpottaa huomattavasti palvelimen etähallinta. Tällä tavoin voidaan ottaa etäyhteys esimerkiksi Windowsin Remote Desktop -ohjelmalla. Ensiksi täytyy kuitenkin mahdollistaa etätyöpöytäyhteys palvelimelta, joka onnistuu Server Managerissa valitsemalla haluttu palvelin, joka olisi tässä tapauksessa ”Local Server”. Palvelimen ominaisuuksista löydetään nopeasti ”Remote Desktop” -kohta, joka ei ole käytössä. (Kuva 20).



Kuva 20 Remote Desktop Server Managerissa

Tähän vaihdetaan ”Allow remote connections to this computer” ja suosituksena on käyttää NLA-autentikointia, jonka on tarkoitus vähentää palvelimen kuormitusta ja vähentää DOS-hyökkäysten riskiä (Kuva 21). Tietoturvan lisäämiseksi on olemassa Remote Desktop Users -ryhmä, jolla voidaan rajoittaa etätyöpöytäyhteyksiä. Ryhmään on lisätty vain Domain Admin -käyttäjä, joten peruskäyttäjät eivät voi ottaa etätyöpöytäyhteyttä.



Kuva 21 Remote Desktop määritykset

Tämän jälkeen palvelimeen voi ottaa etätyöpöytäyhteyden saman verkon sisällä olevasta tietokoneesta Domain Admin -käyttäjän tiedoilla.

5 CLIENT-LAITTEEN MÄÄRITYKSET

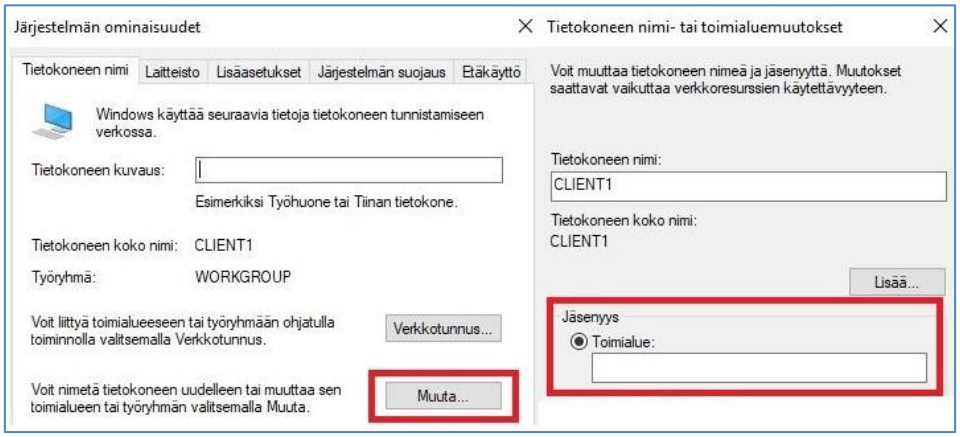
Palvelin on tässä vaiheessa käyttövalmiina, container-osuutta lukuun ottamatta, joten voidaan siirtyä väliaikaisesti tekemään client-puolen määrityksiä. Client-laite nostetaan ensiksi toimialueelle ja sitten määritetään päivitykset tulemaan WSUS:in kautta.

5.1 Client-laitteiden liittäminen domainiin

Client-laitteiden liittäminen tapahtuu Windowsissa polussa ”Ohjauspaneeli\Järjestelmä ja suojaus\Järjestelmä”. Tässä vaiheessa lisätään ”CLIENT1”-niminen laite toimialueelle valitsemalla ”Muuta asetuksia”. (Kuva 22).

Kuva 22 Tietokoneen nimi ja toimialueen asetukset

Painetaan ”Muuta….”-painiketta, josta päästään valitsemaan toimialueen, jonka kenttään kirjoitetaan ”ad.organisaatio.fi”. Tämän jälkeen Windows kysyy toimialueen käyttäjää ja salasanaa, jossa voidaan hyödyntää esimerkiksi testikäyttäjän tietoja. Tietokone täytyy käynnistää uudelleen, jotta muutokset astuvat voimaan. (Kuva 23).



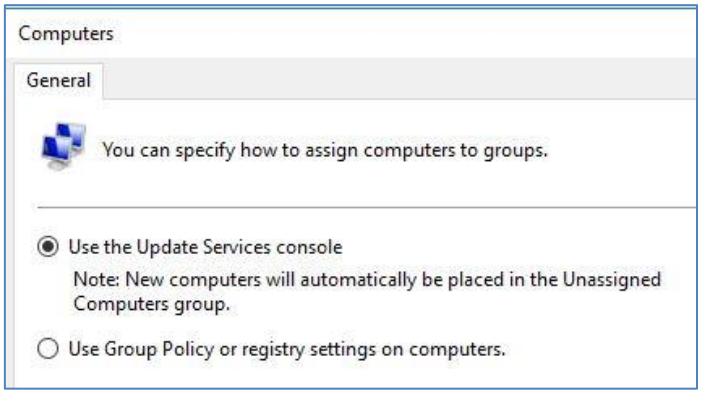
Kuva 23 Toimialueeseen liittyminen

Uudelleenkäynnistyksen jälkeen valitaan ”Toinen käyttäjä”, jos testikäyttäjä ei ole tarjolla, jonka jälkeen kirjautumistietojen alapuolella pitäisi lukea toimialue tai toimialueen NetBIOS-nimi, jolle kirjaudutaan. Tämä tarkoittaa, että laite on onnistuneesti liitetty toimialueeseen. Seuraavaksi kirjaudutaan sisään testikäyttäjällä ja testataan, että käyttäjien kirjautuminen toimii.

Kannattaa huomioida, että, joissain tilanteissa voi tarvita paikallista käyttäjätiliä, jolle pääsee kirjautumaan toimialueelle liitetyllä laitteella, kun kirjoittaa ”**.**” ennen paikallisen käyttäjän nimeä, esimerkiksi ”**.\Administrator**”.

5.2 Windows Server Update Servicesin määritys laitteille

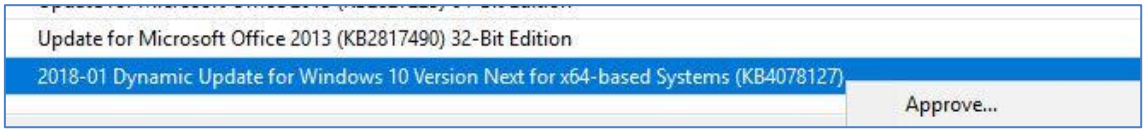
WSUS:in asennuksen jälkeen sille tarvitsee vielä määrittää, mitkä laitteet saavat päivitykset ja millä tavoin ne jaetaan. Tässä tapauksessa tehdään yksinkertainen määritys, jossa WSUS ei käytä Group Policyitä päivitysten jakamiseen, sillä tietokoneympäristö ei ole tarpeeksi suuri sitä varten, joten käytetään siis Update Service consolea päivitysten-hallintaan. Tämän voi varmistaa menemällä: Update Services → Options → Computers. Tässä tarkistetaan, ettei WSUS käytä Group Policyitä (Kuva 24).



Kuva 24 Tietokoneiden ryhmittelyn valinta

Oletuksena tietokoneet ovat Unassigned Computers ryhmässä, jonka takia järjestelmänvalvojan kannattaa luoda haluamansa tietokoneryhmät ”All Computers”-osioon valitsemalla ”Add Computer Group”. Luodaan esimerkiksi Update-niminen tietokoneryhmä, jonne lisätään CLIENT1-laite. Valitaan CLIENT1 laitteen kohdalla ”Change Membership…” ja valitaan Update-ryhmä. Ryhmiä luomalla ja niihin laitteita lisäämällä voidaan hallita useamman koneen päivityksiä ryhmittäin.

Tämän jälkeen Updates-kohdasta voidaan valita, minkälaisia päivityksiä halutaan hyväksyä kullekin laiteryhmälle. Seuraavaksi hyväksytään halutut päivitykset valitsemalla esimerkiksi Critical Updates -kohdasta jokin päivitys hyväksyttäväksi. (Kuva 25).

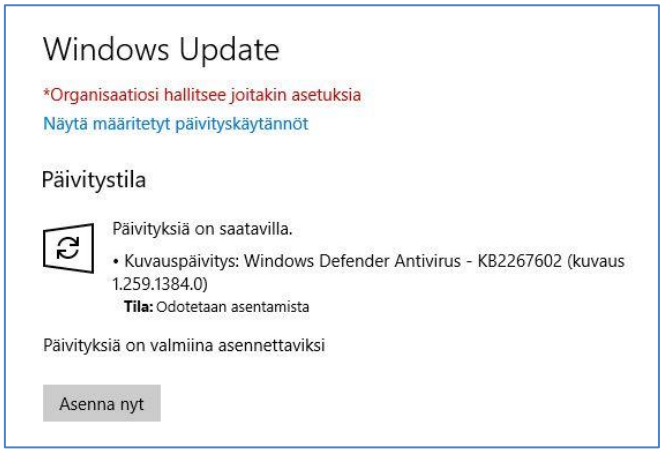


Kuva 25 Päivityksen hyväksyminen

Tämän jälkeen aukeaa valintaikkuna, jossa voidaan valita, mille kaikille ryhmille halutut päivitykset asennetaan (Kuva 26).

Kuva 26 Ryhmän valinta

Seuraavaksi tarkistetaan CLIENT1-laitteen Windows Update, jossa pitäisi lukea, että päivitykset ovat Organisaation hallinnassa ja suorittamalla päivitysten hakeminen hyväksytyt päivitykset latautuvat jonkin ajan kuluessa niiden hyväksymisestä. (Kuva 27).



Kuva 27 Client laitteen Windows Update

5.3 **Containerit**

Lopuksi keskitytään Containereihin, jossa luodaan säiliö käyttäen Powershelliä ja Dockeria. Tätä varten täytyy asentaa Hyper-V ja Container -ominaisuudet palvelimelle käyttäen Add Roles and Features Wizardia, jossa Hyper-V löytyy roolien puolelta (Roles) ja containerit ominaisuuksien (Features) puolelta. Asennuksen jälkeen palvelin käynnistetään uudelleen ja avataan PowerShell varmuuden vuoksi järjestelmänvalvojana, jonka jälkeen asennetaan kaikki tarvittava Dockeria varten. Ajetaan seuraavat komennot PowerShellissä, joilla valmistellaan palvelin Dockeria varten:

Install-Module -Name DockerMsftProvider -Repository PSGallery -Force
Import-Module -Name DockerMsftProvider -Force
Import-Packageprovider -Name DockerMsftProvider -Force
Install-Package -Name docker -ProviderName DockerMsftProvider -Verbose
Install-Package -Name docker -ProviderName DockerMsftProvider -Verbose -Update
Register-PackageSource -ProviderName DockerMsftProvider -Name AlternateSource -Location https://contoso.com/metaData.json

Restart-Computer -Force

Siirrytään polkuun, minne Docker on asennettu (oletuksena C:\Program Files\Docker):

cd 'C:\Program Files\Docker\'

Tämän jälkeen voidaan ajaa Docker-komentoja PowerShellissä:

dockerd.exe
docker version

Jos kaikki on tähän mennessä mennyt oikein, pitäisi Dockerin olla käynnissä. Varmistetaan, että Hyper-V ominaisuus käynnistyy:

Install-WindowsFeature hyper-v

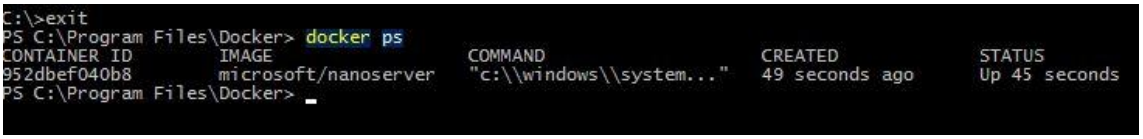
Seuraavaksi asennetaan Windows Nano Serverin base image pull komennolla:

docker pull microsoft/nanoserver

Tämän jälkeen containerin voi käynnistää komennolla:

docker run -i -t microsoft/nanoserver

Tämän kylkeen kannattaa varmistaa uudessa PowerShell istunnossa, että container on käynnissä komennolla **docker ps** (Kuva 28).



Kuva 28 Käynnistettyjen containereiden tarkistus

5.4 IIS:n ajaminen Windows Containerissa

Tässä vaiheessa Dockerissa ilmeni pieniä ongelmia, joiden vuoksi täytyi Docker ja Container-ominaisuudet asentaa uudestaan, mutta tämä ei vie liikaa aikaa, sillä Dockerin saa poistettua komennoilla:

Uninstall-Module dockermsftprovider
Uninstall-Package docker -ProviderName dockermsftprovider

Komentojen lisäksi palvelin täytyy käynnistää uudelleen ja varmistaa, että ”Containers” Windows-ominaisuus on poissa käytöstä Server Managerissa. Tämän jälkeen voidaan taas asentaa Docker uudestaan:

Install-Module -Name DockerMsftProvider -Repository PSGallery -Force
Install-Package -Name docker -ProviderName DockerMsftProvider

Tässä kohtaa kannattaa myös varmistaa, että ”Containers” ominaisuus on päällä.

Tämän jälkeen katsotaan, lähteekö IIS pyörimään Containerissa:

Docker run -it --name nano2 -p 80:80 nanoserver/iis

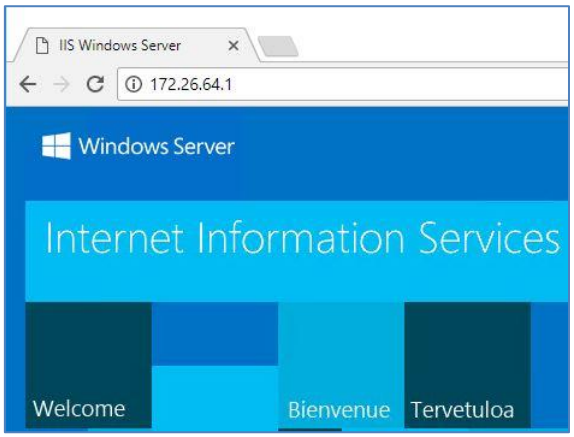
Tarkistetaan mikä on Containerin sisäinen IP-osoite:

ipconfig

Tämän voi myös tarkistaa Containerin ulkopuolelta, kun laittaa komennon:
docker inspect -f "{{ .NetworkSettings.Networks.nat.IPAddress }}" nano2

Edellisessä komennossa ”nano2” on käynnissä olevan Containerin nimi.
IP-osoite täytyy saada selville, koska toistaiseksi olemassa olevan bugin takia, joka vaikuttaa Windowsin tapaan kommunikoida Containereiden kanssa NAT:in välityksellä.

Nämä komennot antoivat sisäiseksi IP-osoitteeksi 172.26.64.1, joka voidaan kirjoittaa Container Host -laitteen selainriville, jonka pitäisi antaa IIS:n etusivu (Kuva 29).

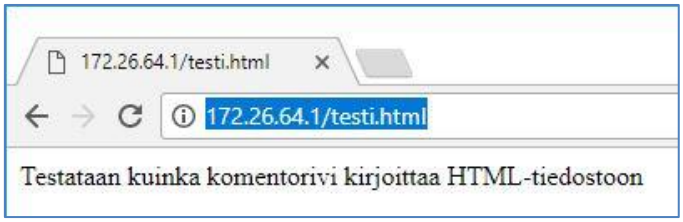


Kuva 29 Containerissa ajetun IIS:n default sivu

Web-palvelimelle voidaan luoda sivuja suuntaamalla Containerissa polkuun ”C:\inetpub\wwwroot>”. Luodaan tänne esimerkiksi HTML-tiedosto, jonka pitäisi aueta selaimessa. Kirjoitetaan seuraava komento Containerin polussa C:\inetpub\wwwroot:

echo Testataan kuinka komentorivi kirjoittaa HTML-tiedostoon > testi.html

Tämän jälkeen, jos siirtyy selaimessa http://172.26.64.1/testi.html, pitäisi päästä käsiksi luotuun HTML-tiedostoon (Kuva 30). Tämä ei kuitenkaan ole kovin tehokas tapa luoda nettisivuja, mutta tällä tavoin voidaan näyttää, kuinka nopeasti Containerilla voidaan luoda asioita.



Kuva 30 Esimerkki HTML-tiedosto

6 JOHTOPÄÄTÖKSET

Jo pienemmissä yrityksissä on erittäin suositeltavaa käyttää palvelinta työasemien, käyttäjien ja resurssien hallinnointiin, eikä niiden käyttöönottoon kulu montaa työtuntia, kunhan suunnittelee etukäteen tarvittavat ryhmät ja käytännöt (OU:t ja Group Policyt). Palvelimen käyttö myöskin helpottaa selvästi IT-ylläpidon työtä, kun käyttäjille voidaan määrittää oikeuksia tarpeen mukaan tiettyihin resursseihin, joita ei tarvitse manuaalisesti määrittää käyttäjäkohtaisesti jokaiselle laitteelle. Myöskin salasanojen unohtaminen ei ole ongelma, kun palvelimen päässä AD:lla voi valita käyttäjän kohdalla ”Reset password”, joka on osoittautunut isommissa yrityksissä ongelmaksi etenkin pitempien lomien päätteeksi. Tällä hetkellä Microsoft pyrkii kehittämään heidän pilvipalveluitaan, siten että Active Directorynkin saisi siirrettyä pilveen, mutta tämä ei ole ainakaan tällä hetkellä täysin mahdollista.

Palvelimen asennus ja käyttöönotto oli melko yksinkertaista ja netistä löytyvillä ohjeilla pääsee pitkälle, mutta olisi hyvä, että on tietämystä etukäteen, mitä lähtee tekemään. Varsinkin WSUS, DHCP ja DNS voivat aiheuttaa ongelmia, jos ei tiedä niistä etukäteen.

Container-tekniikka osoittautui nopeaksi vastineeksi perinteisen virtualisoinnin rinnalle, mutta Windowsin puolella tämä on vielä alkuvaiheessa, verrattuna Linuxin LXC-tekniikkaan. Lähivuosina tämä tilanne varmasti paranee, mutta tällä hetkellä on helpompaa käyttää LXC-tekniikkaa ja perinteistä virtualisointia verrattuna Windows Containereihin, sillä netistä löytyy paljon ohjeita ja valmiita ratkaisuja näihin, eikä tarvitse liiallista opettelua. Ongelmaksi kuitenkin voi muodostua containerin ja host-laitteen välinen kommunikointi, joka voi aiheuttaa ongelmia.

7 LÄHDELUETTELO

Beal, V. (n.d.). Domain. Haettu 15.11.2017 osoitteesta: https://www.webopedia.com/TERM/D/domain.html

Chance, E. (8.8.2016). DOCKER: EXPLAINED SIMPLY. Haettu 15.11.2017 osoitteesta: http://elliot.land/post/docker-explained-simply

Corrie, B. (16.5.2017). What is a Container: Youtube. Haettu 15.11.2017 osoitteesta: https://www.youtube.com/watch?v=EnJ7qX9fkcU

Docker Inc. (n.d.). Dockerfile reference. Haettu 15.11.2017 osoitteesta: https://docs.docker.com/engine/reference/builder/

Docker Inc. (n.d.). Repositories on Docker Hub. Haettu 15.11.2017 osoitteesta: https://docs.docker.com/docker-hub/repos/

Eli the Computer Guy. (22. Helmikuu 2013a). Introduction to Active Directory Directory Services Structure in Windows Server 2012. Haettu 15.11.2017 osoitteesta: https://www.youtube.com/watch?v=lFwek_OuYZ8&

Eli the Computer Guy. (22. Helmikuu 2013b). Introduction to DHCP. Haettu 15.11.2017 osoitteesta: https://www.youtube.com/watch?v=g7mroO_BLD0

Eli the Computer Guy. (22. Helmikuu 2013c). Introduction to DNS (Domain Name Services). Haettu 15.11.2017 osoitteesta: https://www.youtube.com/watch?v=VwpP8PUzqLw&t=

Leonhard, W. (4. Elokuu 2016). The case against Windows 10 Anniversary Update grows. Haettu 15.11.2017 osoitteesta: https://www.computerworld.com/article/3104389/microsoft-windows/the-case-against-windows-10-anniversary-update-grows.html

Marra, M. (27. Marraskuu 2012). Why you shouldn't use .local in your Active Directory domain name. Haettu 15.11.2017 osoitteesta: http://www.mdmarra.com/2012/11/why-you-shouldnt-use-local-in-your.html

Microsoft Corporation. (28. Maaliskuu 2003). How DHCP Technology Works. Haettu 15.11.2017 osoitteesta: https://technet.microsoft.com/en-us/library/cc780760(v=ws.10).aspx

Microsoft Corporation. (23. Huhtikuu 2009). AD DS: All domains should have at least two functioning domain controllers for redundancy. Haettu 15.11.2017 osoitteesta: https://technet.microsoft.com/en-us/library/dd378865(v=ws.10).aspx

Microsoft Corporation. (6. Syyskuu 2013). Microsoft Virtual Academy: Understanding Active Directory. Haettu 15.11.2017 osoitteesta: https://mva.microsoft.com/en-us/training-courses/understanding-active-directory-8233?l=aErw3QJy_6904984382

Microsoft Corporation. (5. Toukokuu 2016a). Virtualization: Windows Containers. Haettu 15.11.2017 osoitteesta: https://docs.microsoft.com/en-us/virtualization/windowscontainers/about/

Microsoft Corporation. (13. Syyskuu 2016b). Virtualization: Hyper-V Containers. Haettu 15.11.2017 osoitteesta: https://docs.microsoft.com/en-us/virtualization/windowscontainers/manage-containers/hyperv-container

Microsoft Corporation. (16. Syyskuu 2016c). Introducing IIS on Nano Server. Haettu 15.11.2017 osoitteesta: https://docs.microsoft.com/en-us/iis/get-started/whats-new-in-iis-10/introducing-iis-on-nano-server

Microsoft Corporation. (16. Syyskuu 2016d). Windows Containers on Windows 10. Haettu 15.11.2017 osoitteesta: https://docs.microsoft.com/en-us/virtualization/windowscontainers/quick-start/quick-start-windows-10

Microsoft Corporation. (15. Marras 2017a). DNS. Haettu 15.11.2017 osoitteesta: https://technet.microsoft.com/en-us/library/cc730921(v=ws.11).aspx

Microsoft Corporation. (14. Marraskuu 2017b). Install Nano Server. Haettu 15.11.2017 osoitteesta: https://docs.microsoft.com/en-us/windows-server/get-started/getting-started-with-nano-server

Microsoft Corporation. (22. Toukokuu 2017c). Windows Server Update Services (WSUS). Haettu 15.11.2017 osoitteesta: https://docs.microsoft.com/en-us/windows-server/administration/windows-server-update-services/get-started/windows-server-update-services-wsus

Perlow, J. (22. Kesäkuu 2017). How containers will transform Windows 10 in the next three years. Zdnet. Haettu 14.5.2018 osoitteesta: http://www.zdnet.com/article/how-containers-will-transform-windows-10-in-the-next-three-years/

Scherer, S. (24. Syyskuu 2016). Run Linux and Windows Containers on Windows 10. Haettu 15.11.2017 osoitteesta: https://stefanscherer.github.io/run-linux-and-windows-containers-on-windows-10/

Sumastre, M. G. (27. Helmikuu 2013). Virtualization 101: What is a Hypervisor? Haettu 15.11.2017 osoitteesta: https://www.pluralsight.com/blog/it-ops/what-is-hypervisor

Wang, C. (29. Kesäkuu 2017). What is Docker? Linux containers explained. Haettu 15.11.2017 osoitteesta: https://www.infoworld.com/article/3204171/linux/what-is-docker-linux-containers-explained.html

Wikipedia. (2017a). Active Directory. Haettu 8.11.2017 osoitteesta: https://fi.wikipedia.org/wiki/Active_Directory

Wikipedia. (2017b). Linux namespaces. Haettu 9.11.2017 osoitteesta: https://en.wikipedia.org/wiki/Linux_namespaces

Wikipedia. (2017c). Cgroups. Haettu 9.11.2017 osoitteesta: https://en.wikipedia.org/wiki/Cgroups

Wikipedia. (2017d). Docker Software. Haettu 8.11.2017 osoitteesta: https://en.wikipedia.org/wiki/Docker_(software)